



**LANGLEY
POLICY
DIRECTIVE**

**Directive: LAPD 2810.1
Effective Date: May 12, 2005
Expiration Date: April 11, 2009**

Responsible Office: Office of Chief Information Officer

SUBJECT: Security of Information Technology (revised 4/28/06)

1. POLICY

It is the policy of NASA Langley Research Center (LaRC) to:

a. Comply with NASA and Federal regulations on prohibited use of IT resources.

b. Ensure that IT resources are used only for official Government business, emergencies, or authorized personal use. Use of the NASA Internet address of "nasa.gov" is a representation of the Agency, analogous to the use of NASA letterhead in which the opinions expressed reflect on NASA. As set forth below, limited personal use of IT resources owned by or operated on behalf of LaRC is considered to be an "authorized use" of those resources.

(1) IT resources owned by or operated on behalf of LaRC are provided for official business. Official Government business broadly includes any computer processing and communications that are required as part of the job. Official business includes, but is not limited to, the performance of NASA work-related duties in position descriptions, professional training and class work, work covered under grant agreements with NASA, tasks directed via NASA contracts, agreements with international partners, and support activities related to NASA contract tasking.

(2) LaRC management considers certain other activities to be within the scope of official business. For example, electronic mail (e-mail) or web sites being used to distribute information about the following:

(a) Work-related events, such as technical symposiums, classes, and presentations.

(b) Activities sponsored by LaRC, such as the child daycare center and carpooling.

(c) Events and activities specific to a particular LaRC organization.

(d) LaRC sanctioned activities, such as blood drives, clubs, and organizations.

(3) Since there is no measurable additional cost, some limited personal use of Internet services, such as the World Wide Web (WWW), is permitted, provided it does not interfere with the employee's work or the work of others. Extreme care must be taken regarding content matter. Use must be kept to brief periods when it can reasonably be assumed that the employee is in a non-duty status, such as during lunch breaks. However, extensive personal access to the Internet via the WWW on computers connected to LaRCNET is not appropriate.

(4) Under no circumstances is it permissible to intentionally access, download, or send material that would create a hostile or offensive work environment, such as racist or sexually explicit material.

(5) Personal use of e-mail is authorized under conditions similar to those for personal use of telephones. However, extensive personal use of e-mail on computers connected to the Langley network (LaRCNET) is not appropriate. When communications cannot reasonably be made during non-business hours or in emergency situations, employees may exchange brief e-mail messages with the following:

- (a) Spouse or dependent.
- (b) Someone responsible for the care of a spouse or dependent.
- (c) Local, state, or federal government agencies.
- (d) Physicians, dentists, and other medical practitioners.
- (e) Businesses, such as those associated with home or auto repair.

(6) The reception of commercial television broadcasts over the network is not permitted because of the drain on network resources.

c. Use IT resources owned by or operated on behalf of LaRC in a responsible manner so as not to place other IT resources at risk. Users of IT resources connected to the LaRC network (LaRCNET) shall:

- (1) Be authorized and sponsored by a LaRC organization.
- (2) Maintain a valid e-mail account on the LaRC e-mail post office.
- (3) Select unique, non-trivial passwords. Unless restricted by hardware or software limitations on the host computer, the password shall have at least eight characters to include characters from the four character sets (upper case letters, lower case letters, numerals, and special characters). Passwords shall not be shared with anyone. Passwords shall be protected from any form of disclosure, to include but not limited to the following: stored in clear-text files; saved in function keys; and remembered by applications, such as terminal logins, e-mail clients or dial-up access. Passwords shall be changed on a regular basis (at least every three months) commensurate with the NASA policy on the protection of the category of information stored or processed on the host computer.
- (4) Report any computer security weaknesses, incidents of possible misuse, or suspected unauthorized access to line managers, system administrators, or the LaRC

IT Security Manager (ITSM). Report all suspected IT security (ITS) incidents or possible inappropriate use in a timely manner by telephone and not by electronic mail (e-mail), unless the message is encrypted. (See LMS-CP-5549, "Responding to Reports of Information Technology Security (ITS) Incidents and Inappropriate Activity.")

(5) Not download, install, or run security programs or utilities that may reveal any weaknesses or vulnerabilities in system security, such as but not limited to sniffers, scanners or password cracking programs without the permission of the LaRC ITSM.

(6) Not divulge access information such as but not limited to modem phone numbers or lists of accounts of users.

(7) Under no circumstances perform any moves, additions, alterations, or replacement of any LaRCNET connections, cable plant, or any other associated equipment. Associated equipment includes, but is not limited to routers, switches, hubs, firewalls, virtual private networks, network intrusion detection systems, modems and wireless connections.

(8) Not intentionally engage in activities to:

(a) Harass other users.

(b) Degrade system or network performance.

(c) Deprive an authorized user access to an IT resource.

(d) Circumvent computer security measures.

(e) Attempt to gain access to data or systems for which proper authorization has not been granted.

(9) Not engage in prohibited activities, to include but not be limited to:

(a) Downloading, creating, viewing, storing or transmitting material that is illegal or offensive to fellow employees or the public, such as but not limited to: hate or racist speech, pornography, gambling, illegal weapons, or terrorism.

(b) Maintaining or conducting an outside business.

(c) Fund raising for charitable organizations.

(d) Monitoring network traffic (e.g., run a sniffer) without prior authorization.

(e) Participating in Chat Rooms, News Groups, or similar activities, which are not official business, related to official duties, or an authorized activity.

(f) Advertising goods or services for sale for monetary or personal gain.

- (g) Sending chain letters, personal mass mailings, hoaxes, or harassing messages.
- (h) Gaining unauthorized access to other computer systems or information.

(10) Users should be particularly careful about using NASA computer systems in any way that could be interpreted as intending to influence any member of Congress to favor or oppose any legislation or appropriation. If the offender is an officer or employee of the United States, such an act may fall under a provision of Title 18 U. S. Code, Section 1913, "Lobbying with appropriated monies," which carries severe penalties upon conviction. If there are any questions about any aspect of this provision of law, contact the LaRC Office of Chief Counsel for advice and assistance.

d. Ensure that all outgoing e-mails or file transfers to non-U.S. persons in the United States or abroad comply with U.S. export control laws, regulations, and NASA export control policy (see LMS-CP-1725).

e. Comply with prescribing NASA and Federal regulations on ITS to ensure adequate protective measures, risk analysis, risk assessments and IT system security plans are in place for all IT resources owned by or operated on behalf of LaRC.

f. Ensure that all IT resources physically connected to LaRCNET meet minimal ITS standards as defined by the LaRC ITSM to include, but not be limited to:

(1) Display the NASA Chief Information Officer's warning banner on all computer access ports that require authentication.

(2) Have an assigned and NASA-certified system administrator, with responsibility for the security configuration of the computer.

(3) Be assigned to an IT system security plan.

(4) Have ITS patches installed in an expeditious manner or as directed by the LaRC Office of CIO.

(5) Maintain current LaRC-supported anti-virus software (for Window-based personal computers and Apple computers) that is configured for automatic downloading of the latest virus definition files, scanning of every file when it is opened, and periodic scans of the entire hard drive on the computer.

(6) Ensure that software packages required by the NASA or LaRC CIO are installed on all compatible systems, unless a written waiver request has been approved.

(7) Ensure that all desktop computers are in compliance with NASA STD 2804, unless a written waiver request has been approved.

(8) Enforce the creation of passwords that conform to NASA policy, where possible; otherwise periodically verify that passwords conform to NASA policy.

- (9) Have regular, periodic back-ups and periodic verification of the ability to restore files from back-ups.
- (10) Disable the automatic start-up of network services that are not utilized.
- (11) Restrict access to the system to the greatest extent possible, to include but not be limited to the use of TCP wrappers on UNIX systems, access control lists, and elimination of default vendor accounts.
- (12) Restrict file sharing to the maximum extent possible.
- (13) Have system logging enabled and have the logs reviewed periodically (weekly as a minimum) for unauthorized access or suspicious activity.
- (14) Use Government approved encryption software to protect administratively controlled information (including but not limited to Privacy Act, export controlled, or company proprietary) while in transit over a network, which includes back-up or archival storage

g. Prohibit the following activities:

- (1) Permanent connection of any IT resource to LaRCNET without ensuring that it meets the minimal ITS standards by having the system scanned for vulnerabilities. Vulnerabilities discovered by the scan shall be corrected or mitigated before the system is utilized in production.
- (2) Establishment or maintenance of any Microsoft Windows domain without the explicit written approval of the LaRC CIO.
- (3) Download, installation or execution of any peer-to-peer file sharing software to share illicit or pirated works, including but not limited to software, music and video.
- (4) Granting foreign nationals or foreign representatives accounts on IT resources owned by or operated on behalf of LaRC, and without concurrence by the LaRC Chief Information Officer and Chief of Security. (See LMS-CP-5518, "Granting Foreign Nationals and Foreign Representatives Computer Accounts.")
- (5) Download of any copyrighted works, including but not limited to software, music and video, for which licensing has not been acquired.

h. Prohibit the following activities, without the explicit written permission of the LaRC ITSM:

- (1) Utilization of non-routable internet protocol (IP) addresses
- (2) Using a single IP address for multiple computers.

- (3) Connection of non-LaRC owned IT resources to LaRCNET, except for IT resources owned and operated by LaRC contractors in support of LaRC.
- (4) Connection, other than by the Network and Computer Services Branch (See LAPD 2400.3), of any network communications devices to LaRCNET, including but not limited to routers, switches, hubs, concentrators, firewalls, virtual private networks, modems or wireless access points.
- (5) Connection of any IT resource on LaRCNET to any external network through a direct physical or wireless link to include modems, except for those computers that comprise the LaRC Remote Access (LaRA) system and the computers of the LaRA support staff for testing remote access.
- (6) Execution of any program to analyze network traffic, except by personnel who are responsible for the maintenance and/or security of LaRCNET.
- (7) Download installation or execution of any freeware, shareware, public domain and/or commercial software from any foreign site, bulletin board, university, Internet service provider or any other non-commercial or non-U.S. Government site, to include but not be limited to software, music, and video.
 - i. Download and install software if and only if the software has been evaluated for correctness of execution and/or is available from NASA, another U.S. Government agency or reputable commercial vendor site within the United States.
 - j. Comply with prescribing documentation on the operation of a registration authority to support the NASA PKI.
 - k. Ensure that all civil servant employees obtain, use and protect their PKI private encryption and digital signature keys in accordance with NASA policy.
 - l. Non-compliance with this LAPD may result in a charge to the organization for restoration of service, a loss of access to LaRC IT resources, disciplinary actions or criminal prosecution.
 - m. Ultimately all NASA and Contractor employees are individually responsible and accountable for proper and legal use of IT resources owned by or operated on behalf of LaRC. This includes personal computers being used for remote connectivity to LaRC, either via the VPN, dial-in remote access server or over a high-speed private Internet service provider. Users of LaRCNET are also collectively responsible for protecting the public's confidence and financial investment in NASA.

2. APPLICABILITY

This LAPD applies to all LaRC employees, all LaRC contractor and subcontractor employees, and all other individuals authorized access to IT resources, that are owned by or operated on behalf of LaRC.

3. AUTHORITY

- a. NPD 2810.1, "Security of Information Technology."
- b. NPD 2540.1D, "Use of Government Telephones"

4. REFERENCES

- a. NPR 1600.1, "NASA Security Program Procedural Requirements "
- b. NPR 2810.1, "Security of Information Technology."
- c. NITR-2810-1, "Agency Wireless Guidelines"
- d. NASA-STD-2804, "Minimum Office Automation Software Suite Interface Standards and Product Standards
- e. NASA Public Key Infrastructure Practices
- f. NASA PKI Registration Authority (RA) Operations Manual
- g. NASA PKI Registration Authority (RA) Operational Readiness Requirements
- h. X.509 Certificate Policy for National Aeronautics and Space Administration (NASA) Public Key Infrastructure (PKI)
- i. LAPD 2400.3, "Langley Research Center (LaRC) Computer Networks for Data Communications"
- j. LMS-CP-1725, "Export Control."
- k. LMS-CP-5518, "Granting Foreign Nationals and Foreign Representatives Computer Accounts."
- l. LMS-CP-5549, "Responding to Reports of Information Technology Security (ITS) Incidents and Inappropriate Activity."
- m. LMS-CP-5630, "Requesting, Modifying, or Restoring a Public Key Infrastructure (PKI) Certificate."
- n. LMS-CP-5631, "Suspending or Revoking a Public Key Infrastructure (PKI) Certificate."

5. RESPONSIBILITIES

Specific responsibilities of individuals and organizations with regard to: (1) the appropriate use of IT resources owned by or operated on behalf of LaRC; (2) the minimum ITS requirements for LaRCNET; (3) the operation of the Registration Authority; and (4) the proper use of PKI certificates are as follows:

a. LaRC Chief Information Officer

- (1) Approve, issue, and implements LaRC ITS policies, procedural requirements, and guidelines.
- (2) Approves or denies access to LaRC IT resources for foreign nationals and foreign representatives.
- (3) Appoints a Network Configuration Control Board.
- (4) Resolves disputes between the LaRC ITSM and supervisors with regard to preventative or corrective actions arising from an ITS incident, or preparation of an IT system security plan.
- (5) Ensures appropriate PKI policies and procedures are issued, communicated and effectively implemented and appoints an Operational Authority for PKI at LaRC.
- (6) With concurrence from the LaRC Office of Chief Counsel, defines limited personal use of the Internet by specifying categories of information to which web access is denied by default, unless the web access is work related.
- (7) Approves appointment of organizational Computer Security Officials (CSOs) and alternate CSOs.
- (8) Ensure that new civil service and contractor employees receive ITS awareness training as a part of their orientation prior to being granted access to LaRC IT resources

b. LaRC Chief of Security

- (1) Approve or deny physical access to LaRC for foreign nationals and foreign representatives.
- (2) Ensure the proper screening of all personnel with access to LaRC IT resources.
- (3) Ensure that LaRC IT policies contribute to the secure operation and protection of IT resources owned by or operated on behalf of LaRC.

c. Network and Computer Services Branch (NSCB), OCIO

- (1) Manage, operate, and deploy LaRCNET.

(2) Terminate LaRCNET access as directed by the LaRC ITSM or his/her designee, when other corrective action is not feasible or has been ineffective.

(3) Restrict access to LaRCNET by external computers or networks as directed by the LaRC ITSM or his/her designee, to protect LaRC from potential hostile activity.

(4) Operate the PKI Registration Authority (RA)

d. LaRC IT Security Manager (ITSM)

(1) Develop LaRC ITS policies, procedural requirements, and guidelines for approval and issuance by the LaRC CIO.

(2) Implement and monitor compliance with LaRC ITS procedural requirements and guidelines.

(3) Investigate suspected ITS incidents or suspected inappropriate use in cooperation with the Office of Human Capital Management, Security Management and Safeguards, Office of Chief Counsel, Inspector General, and appropriate supervisory personnel as required.

(4) Direct LaRCNET personnel to enforce LaRC ITS policies, procedural requirements, and guidelines, to include placing restrictions on the perimeter routers or terminating network access.

(5) Maintain an effective ITS awareness program to include training, briefing, and general ITS information articles or notices to the Center.

(6) Approve appropriate requests for two-factor authentication and VPN accounts.

(7) Ensure an appropriate personnel screening process for granting access to LaRC IT resources.

e. Organizational Development and Workforce Relations Branch, Office of Human Capital Management

(1) Co-ordinate with LaRC ITSM on tracking compliance for annual ITS awareness training.

f. Organizational Unit Managers (OUM)

(1) Designate an organizational Computer Security Official (CSO) and any alternate CSOs in writing to the LaRC ITSM, with approval of the LaRC CIO, and ensure that the CSO duties are addressed in the individual's performance plan.

(2) Ensure that an IT System Security Plan, which includes the assignment of a certified system administrator, a risk assessment, a contingency plan, and certification and accreditation covers every IT resource under the OUM's control.

g. Supervisors

(1) Implement and enforce LaRC's ITS policies for IT resources under their control, to include but not limited to the following:

(a) Systems are scanned regularly for vulnerabilities and corrective measures are implemented expeditiously for any problems discovered.

(b) Designate a person certified for both the operating systems and ITS to have responsibility for ITS for IT resources in the organization.

(2) Review employee use of IT resources and apply internal controls, with an audit trail, as necessary to ensure that only those individuals who require access to IT resources have such access.

(3) Review employee use of IT resources as necessary to ensure that appropriate use of IT resources is strictly enforced and inappropriate use is not tolerated.

(4) Ensure that foreign nationals and foreign representatives are not given accounts except as permitted by LaRC and NASA policy and with the approval of both the LaRC CCS and CIO.

(5) Ensure that information and software is erased from IT resources before excess, transfer, trade-in or disposal.

(6) Ensure that their employees complete annual ITS awareness training.

(7) Validate and approve user requests for PKI and two-factor authentication access.

(8) Responsible for personnel dismissals for cause and reporting those actions, as well as key compromises or suspected compromises to the LaRC ITSM, within 1 hour.

(9) Responsible for personnel terminations, re-assignments or changes in responsibilities that affect PKI and reporting these actions to the LaRC ITSM within 24 hours.

h. Employees

(1) Use IT resources owned by or operated on behalf of LaRC only for official business, emergency, and other approved activities.

(2) Complete ITS awareness training on an annual basis.

(3) Notify supervisor, system administrator and/or LaRC ITSM immediately about any suspected ITS concern, inappropriate use or incident.

(4) Use the PKI in accordance with NASA policy and procedures, including protecting the PKI password from disclosure to any other individual.

(5) Report key compromises or suspected compromises to their supervisor or the LaRC ITSM or the RA within 1 hour.

(6) Comply with all LaRC ITS policies.

i. Contracting Officer's Technical Representative

(1) Responsible for the proper management of IT resource use by contractor personnel.

(2) Ensure proper administration of IT resources connected to LaRCNET that are used or administered by contractor personnel.

(3) Ensure that contractor employees receive annual ITS awareness training.

(4) Ensure that contractor personnel, assigned duties as a system administrator, are certified for all operating systems, which they administer that are covered by the NASA certification program.

(5) Validate contractor requests for PKI or two-factor authentication access.

6. DELEGATION OF AUTHORITY

None

7. MEASUREMENTS

None

8. CANCELLATION

(a) LAPD 2810.1, "Appropriate Use of NASA Langley Research Center Information Technology Resources," dated July 23, 2004

(b) LAPD 2810.2, "Minimum Information Technology Security Requirements for LaRCNET," dated July 23, 2004.

original signed on file

Roy D. Bridges, Jr.
Director